					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P01					Заглавие на документа: **Политика за информационна сигурност**							
Версия: 1.0		Дата на влизане в сила: 01.01.2025			Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго	

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

1. Цел

1.1 Настоящата политика определя общия ангажимент на организацията към информационната сигурност чрез установяване на формална система за управление на информационната сигурност (ISMS).

1.2 Тя определя стратегическата насока и основните изисквания за защита на поверителността, целостта, наличността и устойчивостта на всички информационни активи във физическа, дигитална и облачна среда.

1.3 Политиката изпълнява изискванията на ISO/IEC 27001:2022, клаузи 5.1 и 5.2, като изразява намеренията на ръководството, ангажимента на висшето ръководство и съгласуването на дейностите по сигурност с организационните цели.

1.4 Тя служи като официална отправна точка за всички подчинени политики, стандарти и процедури в рамките на ISMS и представлява съществен елемент за поддържане на среда за сигурност, основана на риска, насочена към съответствие и подлежаща на непрекъснато подобрение.

2. Обхват

2.1 Настоящата политика се прилага за всички лица, активи и процеси, определени в обхвата на ISMS, включително:

2.1.1 Всички бизнес звена, отдели, дъщерни дружества и клонове

2.1.2 Служители, изпълнители, временен персонал, консултанти и външни доставчици на услуги

2.1.3 Всички данни, информационни системи, приложения, инфраструктура и комуникационни канали

2.1.4 Всички физически, облачни, отдалечени и хибридни среди, в които се обработват или до които се осъществява достъп до фирмени данни

2.2 Политиката е задължителна за всички страни, които обработват информация на организацията, и се прилага за всички етапи от жизнения цикъл на информацията — от създаването и предаването до съхранението и унищожаването.

2.3 Всички изключения или ограничения в рамките на този обхват трябва да бъдат документирани в декларацията за обхвата на ISMS и обосновани с официално одобрение от изпълнителното ръководство.

3. Цели

3.1 Да се установи ISMS, съответстваща на ISO/IEC 27001:2022 и способна да подпомага вземането на решения, основано на риска, в цялата организация.

3.2 Да се гарантира, че принципите за поверителност, цялост и наличност са внедрени във всички организационни дейности, системи и партньорства.

3.3 Да се осигури съответствие с регулаторните и договорните изисквания чрез определяне на измерими цели по сигурност, основани на политиката, и чрез интегрирането им в бизнес дейностите.

3.4 Да се сведе до минимум вероятността и въздействието на инциденти по информационна сигурност чрез ефективни превантивни, детективни и коригиращи контроли.

3.5 Да се насърчава непрекъснатото повишаване на зрелостта по информационна сигурност чрез определени показатели за ефективност, резултати от одити и прегледи от ръководството.

3.6 Да се утвърждава култура на отчетност, осведоменост и устойчивост, при която отговорностите по сигурността се разбират и изпълняват от целия персонал.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява и утвърждава Политиката за информационна сигурност и рамката на ISMS.

4.1.2 Осигурява съгласуваност между целите по сигурност и бизнес стратегията.

4.1.3 Дава личен пример и насърчава силна култура на информационна сигурност.

4.1.4 Преглежда и одобрява съществени промени в обхвата на ISMS, третирането на риска и структурата на управление.

4.2 Директор „Информационна сигурност“ (CISO) / Мениджър на ISMS

4.2.1 Отговаря за ISMS и поддържа настоящата политика в съответствие с ISO/IEC 27001.

4.2.2 Ръководи процесите по оценка на риска, внедряване на контроли и непрекъснато подобрение.

4.2.3 Осигурява координация между функциите по сигурност и упражнява надзор върху подчинените политики.

4.2.4 Докладва състоянието на ISMS, инцидентите, резултатите от одити и показателите пред изпълнителното ръководство.

4.2.5 Осигурява извършването на прегледи и актуализации на политиката в съответствие с раздел 9 от настоящия документ.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Изисквания за преглед и актуализация

9.1 Честота на прегледа

9.1.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно или при настъпване на някое от следните основания:

9.1.1.1 Съществени промени в правните, регулаторните или договорните задължения

9.1.1.2 Съществени промени в рисковия профил на организацията

9.1.1.3 Резултати от вътрешни или външни одити

9.1.1.4 Съществени инциденти или откази на контроли

9.2 Отговорност и процес по прегледа

9.2.1 CISO или определен Мениджър на ISMS ръководи процеса по преглед.

9.2.2 Входните данни за прегледа трябва да включват:

9.2.2.1 Резултати от вътрешен одит

9.2.2.2 Тенденции в оценките на риска

9.2.2.3 Промени в бизнес процесите и технологиите

9.2.2.4 Изпълнение спрямо KPI и праговете за риск

9.2.3 Всички актуализации трябва:

9.2.3.1 Да бъдат под управление на версиите и документирани

9.2.3.2 Да бъдат одобрени от изпълнителното ръководство

9.2.3.3 Да бъдат разпространени до всички засегнати страни чрез официалните канали за комуникация

9.2.3.4 Да водят до необходимите актуализации на подчинената документация и обученията

10. Свързани политики и зависимости

10.1 Настоящата основополагаща политика е пряко свързана със следните организационни политики и рамки по сигурност:

10.1.1 P2 – Политика за роли и отговорности по управление: Определя структурата на управление и йерархията на правомощията, към които се препраща в настоящия документ.

10.1.2 P3 – Политика за допустима употреба: Определя изискванията за поведение и допустимото боравене с информационни активи.

10.1.3 P4 – Политика за контрол на достъпа: Операционализира контролите, свързани с достъпа, произтичащи от настоящата рамкова политика.

10.1.4 P6 – Политика за управление на риска: Осигурява контекста, основан на риска, за избор на контроли и приемане на остатъчни рискове.

10.1.5 P33 – Политика за одит и наблюдение на съответствието: Описва как вътрешните механизми за осигуряване валидират прилагането на политиката.

10.2 Тези взаимовръзки осигуряват цялостна съгласуваност и проследимост в рамките на ISMS и подпомагат единното управление на риска и съответствието.

11. Референтни стандарти и рамки

11.1 Настоящата Политика за информационна сигурност е формално съгласувана със следните стандарти и рамки, за да осигури пълно съответствие, готовност за одит и възможност за доказване пред регулаторните органи:

11.2 ISO/IEC 27001

11.2.1 Клауза 5.1 – Лидерство и ангажираност: Настоящата политика демонстрира ангажимента на висшето ръководство към информационната сигурност и определя отговорностите и разпределението на ресурсите за ISMS.

11.2.2 Клауза 5.2 – Политика за информационна сигурност: Настоящият документ служи като официална политика по сигурност на организацията, съгласувана с определените цели по сигурност, бизнес стратегията и съответствието с ISO/IEC 27001.

11.2.3 Клауза 6.1 – Действия за адресиране на рискове и възможности: Подходът, основан на риска, отразен в настоящата политика, гарантира, че ресурсите за сигурност се прилагат съразмерно на заплахите.

11.2.4 Клауза 9.2 – Вътрешен одит и клауза 10 – Подобрение: Настоящата политика е интегрирана в цикъла на непрекъснато подобрение на организацията и подлежи на валидиране чрез вътрешен одит.

11.2.5 ISO/IEC 27002:2022 – Контрол 5.1: Определя насоки за установяване и поддържане на политики по сигурност. Настоящата политика отразява препоръките на ISO/IEC 27002 относно йерархична документация, цикли на преглед и приложимост.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Политика и процедури за планиране на сигурността): Настоящата политика изпълнява изискването за разработване, разпространение и преглед на формална политика за информационна сигурност на организационно ниво.

11.3.2 PM-1 до PM-5: Обхваща управлението на програмно ниво, включително ролите по информационна сигурност, разпределението на ресурси, стратегията за риска и интегрирането на планирането на сигурността в операциите на организацията.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 5(2): Утвърждава принципа на отчетност. Настоящата политика определя отговорните страни и проследимите действия по прилагане.

11.4.2 Член 24: Изисква внедряване на технически и организационни мерки, включително политики, съобразени с риска.

11.4.3 Член 32: Подпомага внедряването на подходящи мерки за гарантиране на сигурността на личните данни през целия им жизнен цикъл.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(a): Задължава организациите да внедрят документирана политика по сигурност, обхващаща управлението на риска и управлението. Настоящата политика изпълнява това изискване и подпомага по-широката киберустойчивост и защитата на критичната инфраструктура.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 5(2): Изисква документирана рамка за вътрешен контрол за управление на ИКТ риска. Настоящата политика подпомага съответствието във финансовия сектор чрез определяне на роли, контроли и надзорни функции, съгласувани с изискванията на DORA относно управлението.

11.7 COBIT 2019

11.7.1 EDM01 – Установяване на рамка за управление: Настоящата политика подпомага корпоративното управление чрез определяне на ролите в ISMS, ангажиментите на ръководството и стратегическите цели.

11.7.2 APO01 – Рамка за управление: Подпомага установяването и функционирането на структурирана ISMS.

11.7.3 APO12 – Управление на риска: Осигурява основата за управление на риска по информационна сигурност.

11.7.4 MEA01/MEA03 – Наблюдение, оценка и преценка: Подсилва непрекъснатата оценка на резултатите и наблюдението на вътрешния контрол чрез прилагане на изискванията на политиката.